The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

5/22/2014

SUBJECT:

Vulnerability in Internet Explorer 8 Could Allow Remote Code Execution

EXECUTIVE SUMMARY:

A vulnerability has been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

It should be noted that there is currently no patch available for this vulnerability. It is currently unknown if it is being exploited in the wild.

SYSTEMS AFFECTED:

- Microsoft Internet Explorer 8

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

A vulnerability has been reported affecting version 8 of Internet Explorer that could allow for remote code execution. This vulnerability exists due to the way that Internet Explorer handles CMarkup objects. Specifically this issue occurs when freeing a CMarkup object from memory after the execution of certain JavaScript code followed by a CollectGarbage call. By manipulating a document's elements an attacker can force a dangling pointer to be reused after it has been freed. An attacker can leverage this vulnerability to execute code under the context of the current process. The vulnerability may corrupt memory in a way that could allow an attacker to execute arbitrary code, in the context of the current user, within Internet Explorer. An attacker could host a specially crafted website designed to take advantage of this vulnerability, and then convince or trick an unsuspecting user to visit their site.

Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

It should be noted that there is currently no patch available for this vulnerability. It is currently unknown if it is being exploited in the wild.

RECOMMENDATIONS:

The following actions should be taken:

- Consider using an alternate browser until a patch is made available for the vulnerable versions of Internet Explorer.
- Consider implementing Microsoft's Enhanced Mitigation Experience Toolkit (EMET) as it has been reported to make the vulnerability difficult to exploit.
- Run Internet Explorer with Protected Mode enabled.
- Set Internet and Local intranet security zone settings to "High".
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Security Focus:

http://www.securityfocus.com/bid/67544

Tippingpoint Zero Day Initiative:

http://zerodayinitiative.com/advisories/ZDI-14-140/

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1770